07-10-00

A

Practitioner's Docket No. MWH-0043US

*PATENT*

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**Box Patent Application**
**Assistant Commissioner for Patents**
**Washington, D.C. 20231**

## NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): Richard S. Judson

For (title): METHODS AND APPARATUS FOR ENSURING THE PRIVACY AND SECURITY OF PERSONAL MEDICAL INFORMATION

### 1. Type of Application

This transmittal is for an original (nonprovisional) application.

### 2. Papers Enclosed

**A.** Required for filing date under 37 C.F.R. 1.53(b) (Regular) or 37 C.F.R. 1.153 (Design) Application

| | | |
|---|---|---|
| Specification | 8 | Page(s) |
| Claims | 4 | Page(s) |
| Abstract | 1 | Page |
| Drawing(s)--Formal | 4 | Page(s) --Formal |

**CERTIFICATION UNDER 37 C.F.R. 1.10***
*(Express Mail label number is **mandatory**.)*
*(Express Mail certification is optional.)*

I hereby certify that this correspondence and the documents referred to as attached therein are being deposited with the United States Postal Service on July 7, 2000 (date), in an envelope as "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 C.F.R. 1.10 Mailing Label Number EK504826719US addressed to Box Patent Applications, Assistant Commissioner for Patents, Washington, D.C. 20231.

Cathy Wilcox
*(type or print name of person mailing paper)*

**Signature of person mailing paper**

*WARNING:* *Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.*

***WARNING:** *Each paper or fee filed by "Express Mail" **must** have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. 1.10(b) "Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will **not** be granted on petition." Notice of Oct. 28, 1996, 60 Fed. Reg. 56,439, at 56,442.*

**B.** Other Papers Enclosed

| | | |
|---|---|---|
| Declaration and Power of Attorney | 2 | Page(s) |
| Return Receipt Postcard | 1 | |
| Small Entity Statement | 1 | Page |
| Recordation Form (Form PTO-1595) | 1 | Page |
| Assignment of Invention | 3 | Page(s) |

## 3. Inventorship Statement

The inventorship for all the claims in this application are:

The same

## 4. Language

English

## 5. Assignment

An Assignment of the invention to Genaissance Pharmaceuticals, Inc.

Enclosed with this New Application Transmittal:

Recordation Form PTO-1595
Assignment of Invention

## 6. Fee Calculation (37 C.F.R. Section 1.16)

CLAIMS AS FILED

| | Number Filed | Provided with Basic Fee | Number Extra | Rate | Basic Fee $690 |
|---|---|---|---|---|---|
| Total Claims | 19 | 20 | 0 | X $ 18.00 | $ .00 |
| Independent Claims | 07 | 3 | 4 | X $ 78.00 | $312.00 |
| Multiple Dependent Claim(s) , if any | 0 | 0 | 0 | X$260.00 | $ . 00 |

Filing Fee Calculation $1,002.00

## 7. Small Entity Statement

Verified statement that this is a filing by a small entity under 37 CFR 1.9 and 1.27 is attached.

Filing Fee Calculation (50% of above) $ 501.00

8. **Fee Payment Being Made at this Time**

Enclosed:

| | |
|---|---|
| Basic Filing Fee | $ 501.00 |
| Total Fees enclosed | $ 501.00 |

9. **Method of Payment of Fees**

Check in the amount of $501.00

10. **Authorization to Charge Additional Fees**

The Commissioner is hereby authorized to charge the following additional fees which may be required to Deposit Account No. 50-1293:

37 CFR 1.16 (filing fees and presentation of extra claims)

37 CFR 1.17 (application processing fees)

A duplicate of this cover sheet is enclosed

11. **Instruction as to Overpayment:**

Credit Deposit Account No. 50-1293

12. **Bar Code Label**

25106
PATENT TRADEMARK OFFICE

Melodie W. Henderson 7/7/2000
Melodie W. Henderson
Registration No. 37,848
GENAISSANCE PHARMACEUTICALS, INC.
Five Science Park
New Haven, Connecticut 06511
(203) 773-1450 (ext. 3021)

**Practitioner's Docket No.** MWH-0043US *PATENT*

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Judson, Richard S.

Title: METHODS AND APPARATUS FOR ENSURING THE PRIVACY AND SECURITY OF PERSONAL MEDICAL INFORMATION GENE

Filed on: July 6, 2000

## STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) and 1.27(b)--SMALL BUSINESS CONCERN

I hereby state that I am :

An official of the small business concern empowered to act on behalf of the concern identified below:

Genaissance Pharmaceuticals, Inc.
Five Science Park
New Haven, CT 06511

I hereby state that the above identified small business concern qualifies as a small business concern, as defined in 13 CFR 121.12, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office under Sections 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third-party or parties controls or has the power to control both.

I hereby state that rights under contract or law have been conveyed to, and remain with, the small business concern identified above, with regard to the invention described in the application identified above.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c), if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each such person, concern or organization is listed below.

FULL NAME Genaissance Pharmaceuticals, Inc.

ADDRESS Five Science Park
New Haven, CT 06511

SMALL BUSINESS CONCERN

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small business entity is no longer appropriate. (37 CFR 1.28(b))

SIGNATURE Jean Bernard Date 7/7/00

# METHODS AND APPARATUS FOR ENSURING THE PRIVACY AND SECURITY OF PERSONAL MEDICAL INFORMATION

## FIELD OF THE INVENTION

This invention relates to methods and devices for ensuring the privacy and security of personal medical information, and in particular to methods and devices for ensuring the privacy and security of personal genetic information.

## BACKGROUND OF THE INVENTION

As knowledge of the human genome increases, an increasing number of genetic markers are being identified as either the cause of, or being associated with, an increased risk of developing various diseases and conditions. Genetic testing for these markers will allow physicians to identify those at risk of developing certain diseases and take action to prevent, or at least reduce the risk of developing, these diseases. It is also possible to test for genetic markers associated with variations in drug response, and to predict how a patient will respond to a particular drug treatment. However, despite the obvious medical benefit, people may be hesitant to permit such testing for fear that they might be discriminated against by prospective employers and insurers due to an increased risk of disease revealed by such a test, or an indication that a patient is not responsive to conventional treatment revealed by such a test. Thus, ensuring the privacy and security of medical information, and particularly genetic testing information, is important to encourage the public to permit such testing.

Some efforts have been made to provide anonymity for medical test results. For example, in the past numbered test kits have been available with which a person can take a sample, such as a blood sample, and mail the sample to the issuing laboratory, and anonymously call in for the test results by referencing the number on the test kit. However in many instances such a patient-initiated testing system is not appropriate, for example where it is not apparent to the patient what type of test to order, where the collection of the sample is not routine or within the ability of the patient, or where the significance of, or interpretation of, the results is not within the ability of patient. This is particularly true for testing for efficacy of certain courses of drug therapy. In these instances, a patient needs the assistance of a health care professional, and may avoid valuable tests out of concern for the privacy and security of the test results.

## SUMMARY OF THE INVENTION

Generally, the method of this invention allows for the private and secure reporting of a patient's medical tests. The method comprises providing the patient with a medical data card (MDC) issued by a secure information provider (e.g., a trusted third party between the patient's physician or healthcare provider and a testing laboratory), and having a unique patient identification number (PID), a public key encryption private key (Key 1), and a public key encryption public key (Key 2). This medical data card may also include provision for storing information about medical tests conducted on the patient, including information about the type of test conducted, a unique identification number for the test, and the results of the test. The patient's medical data card is used to generate a first test request card (REQ1) that accompanies the test specimen taken from the patient to the secure information provider. The first test request card includes an encrypted identification of the patient and the test; a code identifying the health care provider; the patient identification number (PID); public encryption public key (Key 2); and an identification of the test type. The secure information provider uses the first test request card to generate a second test request card (REQ2) to forward the patient's specimen to a testing laboratory. The second test request card and the specimen are forwarded to the laboratory. The second test request card bears an encryption of the patient's unique identification number, but does not otherwise bear any indicia that would identify the patient. The specimen is sent to a laboratory, which performs the tests prescribed by the heath care professional, and generates a first test results card (RES1). The results, together with the patient's unique identification number, are provided to the secure information provider that issued the medical data card. The secure information provider encodes the test results onto a second test results card, and forwards the card to the health care provider. The health care provider can identify the patient from the information on the second test results card (RES2), and contact the patient. The test results on the second test results card can only be read in conjunction with the patient's medical data card. In the preferred embodiment, after reading the results, the results are transferred to the patient's medical data card.

The method and apparatus of the present invention thus allow for the private and secure reporting of medical test results, such as genetic test results. The specimen taken for the testing cannot be identified with a particular patient, during transmission to the laboratory, conduct of the testing, or reporting of the results. The results are provided to a secure information provider, who encodes the information on a test results card that can only be read in conjunction with the patient's medical data card. Even the secure information provider can operate without knowing the actual identity of the patient; although in some embodiments, the secure information provider may have access to both patient identity information and to the test results. Thus, the patient controls who has access to the testing information.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a flow chart of a method of privately and securely reporting medical tests results according to the principles of this invention;

Fig. 2 is a schematic view of the method shown in Fig. 1;

Fig. 3 is a plan view of a medical data card constructed according to the principles of this invention, for use with the method of this invention;

Fig. 4 is a plan view of a first test request card constructed according to the principles of this invention, for use with the method of this invention;

Fig. 5 is a schematic diagram of a reader for reading medical data cards and printing test request cards for use with the method of this invention;

Fig. 6 is a plan view of a second test request card constructed according to the principles of this invention, for use with the method of this invention;

Fig. 7 is a plan view of a first test results card constructed according to the principles of this invention, for use with the method of this invention;

Fig. 8 is a plan view of a second test results card constructed according to the principles of this invention, for use with the method of this; and

Fig. 9 is a schematic view of a reader for reading test results cards and displaying the results, for use with the method of this invention.

Corresponding reference numerals indicate corresponding parts throughout the drawings.

## DETAILED DESCRIPTION OF THE INVENTION

The present invention includes both methods and apparatus for ensuring the privacy and security of personal medical information, including but not limited to genetic testing information. A flow chart of the method of the present invention is shown in Fig. 1, and the method is shown schematically in Fig. 2. In accordance with the preferred embodiment of this invention, a patient would apply to a secure data provider for a medical data card, and would be issued a card. As shown in Fig. 3 and described herein, the MDC 100 is adapted for use in facilitating genetic testing for a predicted clinical outcome, such as susceptibility to disease and/or response to a particular drug therapy. However, the invention is not so limited, and thus, the medical data card could be adapted for other types of medical testing or adapted for both genetic and other medical testing.

The MDC 100 is preferably compact, for example the size of a standard credit card (about 3.4 inches by about 2.1 inches) so that the patient could conveniently carry the card with him or her in a wallet or purse with other medical cards, such as insurance cards. The MDC 100 preferably has identifying indicia 102, such as the patient's name, imprinted or embossed thereon, so that the patient can correctly identify his or her card. The MDC 100 may also include information (not shown), such as the name, address, telephone number, or other contact information about the issuing secure data provider. The MDC 100 preferably also includes a data storage element 104. The data storage element 104 is readable, and preferably both readable and writeable. The data storage element 104 may be, for example, a magnetic stripe or other magnetic media on the card; an embedded memory chip or other electronic storage media, an optically readable and writeable media, or any other suitable element for storing data. In the preferred embodiment, the data storage element 104 is a computer readable and writeable memory chip.

Stored in the memory of the chip of the data storage element 104 is information about the patient and about the tests that have been conducted. In the preferred embodiment this information would include the information shown in Table 1 below:

Table 1 - Information on the MDC

| Field Name | Description |
|---|---|
| PID | Unique patient ID |
| Test Type | Type of the current test |
| Test ID | Unique ID for that test for that patient |
| Results | Results of the test – usually a short string of characters or a yes/no or a +/- |
| Key 1 | Public key encryption private key |
| Key 2 | Public key encryption public key |

As is apparent from the Table 1, in the preferred embodiment the MDC 100 contains a single unique patient identification code (PID), a single unique public key encryption private key (Key 1), and a single unique public encryption public key (Key 2). The MDC 100 is also capable of storing data relating to one or more tests. The data for each test preferably includes data on the test type, a unique identification number or code (ID) for the test, and the results of the test.

As shown in Fig. 1, at 20 a patient with a MDC 100 consults a health care provider, for example a hospital, a clinic, or a private physician's office. As shown in Fig. 1, at 22 if the health care provider prescribes a medical test, such as a genetic test, the health care provider takes the appropriate specimen (e.g., a blood specimen) from the patient, and uses the patient's MDC 100 to prepare a first test request card (REQ1) 200. See Fig. 4. The REQ1 200 will preferably include the information in Table 2 in bar code (BC) format:

Table 2 - Information on the REQ1

| **Field Name** | **Description** |
|---|---|
| BC1 | An encrypted concatenation of the PID, the Test Type, and the Test ID |
| BC2 | A code corresponding to the particular health care provider prescribing the test |
| BC3 | The PID |
| BC4 | Key 2 (the public encryption private key) |
| BC5 | Test type |

The information provided on the REQ1 200 can be stored in any convenient manner, including optically, magnetically, or electrically. In the preferred embodiment the information is printed on the card in bar code form, which is easy to print and easy to read with readily available, relatively inexpensive equipment. The REQ1 could be in the form of a label applied to the container of the specimen, for example on a vial, or on a bag containing the vial, so that the REQ1 can be removed and replaced by the secure data provider as explained below. BC1 is a combination or concatenation of the PID read from the patient's MDC, the test type entered by the health care provider, and a unique test identification number. This number can either be obtained from the secure information provider, or generated by the hardware/software provided by the secure information provider. This combination or concatenation is encrypted using the Key 2 read from the patient's MDC. The BC1 is a unique identifier for this patient-test combination. BC2 is an identification code for the health care provider. This can be an identification code assigned by the secure information provider, or an identification code assigned by some third party, that uniquely identifies the health care provider. BC3 is simply the PID obtained from the patient's MDC. BC4 is the Key 2 obtained from the patient's MDC. BC5 is simply an identification of the type of test prescribed by the health care provider. The REQ1 200 will also have, in plain text, the address of the secure data provider.

At the time that a health care provider prescribes a particular test, and in this preferred embodiment a genetic test, the patient inserts his or her MDC 100 into a reader unit 300 (shown in Fig. 5). The reader unit 300 has a slot 302 into which the MDC 100 can be inserted, to read the data storage in element 104. The reader unit 300 also includes a printer 304 for printing the REQ1 200.

As shown in Fig. 1, at 24, the secure data provider receives the REQ1 200 and the accompanying specimen, and prepares a second test request card (REQ2) 400 that is devoid of any accessible identification of the patient. See Fig. 6. The REQ2 can be in the form of a label that is attached to the container for the specimen, for example a vial, or it can be attached to a bag containing the vial. More specifically, the REQ2 400 includes only BC1, BC4, and BC5 and the address of the secure data provider 402. The secure data provider sends the specimen and the REQ2 400 to a laboratory which conducts the prescribed tests. These can be sent in a plain envelope, so there is nothing on the package to indicate the identity of the patient. BC1 is a unique identifier of the sample, but because it is encrypted the laboratory cannot determine the identity of the patient.

As shown in Fig. 1, at 26, the laboratory then performs the prescribed test (identified to the laboratory in BC5 on the REQ2 400), and encrypts the results (using BC4 on the REQ2 400). The encrypted results are recorded as another bar code, BC6. The laboratory prepares a first test results card (RES1) 500. See Fig. 7. The RES1 500 contains specimen-identifying information (BC1, which is encrypted, from the REQ2 400) and the results (BC6, which is also encrypted), and sends the RES1 500 to the secure data provider, identified at 402 on the REQ2 400.

As shown in Fig. 1, at 28, the secure data provider receives the RES1 500, and identifies the health care provider (BC2) and the patient identifier PIC (BC3) corresponding to the BC1 on the RES1 500. The secure data provider then prepares a second test results card (RES2) 600 containing BC1, BC3, and BC6, and sends the RES2 600 to the health care provider.

As shown in Fig. 1, at 30, the health care provider receives the RES2 600, and using the PID (BC3) on the RES2, looks up the patient contact information, and requests that the patient come in. The patient comes in and brings his/her MDC 100. The patient's MDC 100 is inserted into a reader 700 along with the RES2 600. The reader takes the private key (Key 1) from the MDC 100, decrypts BC1 (to identify the test) and decrypts BC6 (the results). The results of the test is then written to the MDC 100 and displayed on a display for the health care provider's use. The health care provider then makes his/her diagnostic or therapeutic treatment decision based on these results. The decision can be recorded in the patient's permanent record, but the actual test results are not. After the data is transferred from the RES2 600 to the patient's MDC 100, the RES2 600 is erased and discarded, leaving the MDC as the only permanent record of the test results, with a backup at the secure data provider.

In the preferred embodiment, a reader 700 is provided for reading the RES2 600. The reader 700 has two slots 702 and 704 for receiving the MDC 100 and the RES2 600, and a display 706 for displaying the test results. The use of a reader 700 ensures that the patient does not access the test results without proper supervision or explanation from a health care provider.

In the preferred embodiment, after the results are read on the display 706, the information is transferred from the RES2 600 to the storage element 104 of the MDC 100, so that the patient has a record of the information for future use and reference, but there is no other record of the results available that is identified specifically with the patient. The health care professional can then determine a proper course of action based upon the genetic testing results.

Of course, access to the data storage element 104 of the MDC 100 can be protected with a PIN (personal identification number) so that mere access to the MDC 100 alone will not allow access to either the patient's unique identification number and/or to the information stored in the MDC. In this case the readers 300 and 700 would also include keypads 308 and 708, respectively, so that the patient can enter his or her PIN to enable the reader 300 to read the patient's unique PID, or to allow the reader 700 to read the MDC 100 containing the patient's test results. For convenience the reader 300 and the reader 700 could be consolidated into one device.

## OPERATION

A patient applies for and obtains a MDC 100. As illustrated in Fig. 2, at some point a health care provider prescribes a particular genetic test, or other medical test. The patient inserts his or her MDC 100 into the slot 302 of the health care provider's reader 300, keys in his or her PIN, and a REQ1 200 is printed. The health care provider takes the appropriate specimen, for example a blood specimen, and sends the specimen with the REQ1 400 to the secure data provider. The secure data provider prepares a REQ2 400 and forwards the specimen the REQ2 to a laboratory. The laboratory conducts the tests identified on the REQ2 400, and prepares a report RES1 500, and sends the RES1 to the secure data provider. The secure data provider prepares a RES2 600, and forwards it to the health care provider. The patient inserts the MDC 100 into slot 702 of the reader 700, and the RES2 600 into the slot 704 of the reader. The patient keys in his or her PIN on the keypad 708, and the reader 700 decodes the test results stored on the RES2 and displays them on display 806. The reader preferably also transfers the information from the RES2 600 to the element 104 on the MDC 100, so that the patient has a record of the test results. If the information is needed in the future, the patient can bring the MDC to the health care institution, insert it into a reader 700, enter his or her PIN, and access the results of the prior tests. If the MDC 100 is lost or stolen, a duplicate can be assembled from the records maintained by the secure data provider.

While the invention has been described in connection with specific embodiments thereof, it will be understood that it is capable of further modifications and this application is intended to cover any variations, uses, or adaptations of the invention following, in general, the principles of the invention and including such departures from the present disclosure as come within known or customary practice within the art to which the invention pertains and as may be applied to the essential features hereinbefore set forth, and as follows in the scope of the appended claims.

What is Claimed is:

1. A method of ensuring the security of patient's data from medical tests conducted by a third-party, the method comprising:

providing the patient with a medical data card containing a unique patient identification number;

taking a specimen from the patient for conducting the medical test;

generating a first medical test request containing the unique patient identification number using the patient's medical data card, and

transmitting the specimen and the first medical test request to a third party data provider that generates a second medical test request devoid of accessible patient identification information using the first medical test request and transmits the specimen and second medical test to a third party laboratory and receives the results from the laboratory, and reports the results on a test results card that can only be read in conjunction with the patient's medical data card.

2. The method according to claim 1 further comprising reading the test results on the test results card using the patient's medical data card.

3. The method according to claim 1 wherein the patient's medical data card includes a memory, and further comprising the step of storing the test results in the memory on the patient's medical data card.

4. The method according to claim 1 wherein the patient identification number is not readable from the patient's medical data card without a PIN, and wherein the step of generating the first medical test request includes the patient supplying the PIN.

5. The method according to claim 2 wherein the test results are not readable with the medical data card without a PIN, and wherein the step of reading the test results on the test results card includes the patient supplying the PIN.

6. A method of ensuring the security of patient's data from medical tests conducted for a medical provider by a third-party laboratory, the method comprising:

issuing the patient a medical data card containing a unique patient identification number;

receiving from the medical provider a first request for a medical test generated using the patient's medical data card, and a patient specimen for use in conducting the test;

generating a second request for a medical test using the first request for a medical test, the second request for a medical test being devoid of publicly accessible information about the identity of the patient;

forwarding the second request for a medical test and the specimen to a third party laboratory for conducting the test, and receiving the results of the test from the laboratory; and

providing the tests results to the medical provider in a form that can only be read in conjunction with the patient's medical data card.

7. The method of claim 6, wherein the tests results are on a tests results card in computer readable form and the method further comprises providing the medical provider with a reader adapted for reading the tests results.

8. A medical data card for use in a system for ensuring the security of a patient's data from medical tests conducted for a medical provider by a third-party laboratory, the medical data card including a unique patient ID code, a public key encryption private key, and a public key encryption public key, and a data storage element.

9. The medical data card of claim 8, wherein the data storage element is adapted for storing data for at least one test, including for each test: the type of test, a unique identification code for the test, and the results of the test.

10. A test request card for use in a system for ensuring the security of patient's data from medical tests conducted for a medical provider by a third-party laboratory, the test request card including encrypted information identifying the patient, the test type, an identification of the medical provider, a unique patient identification number, and a public encryption public code.

11. The test request card according to claim 10, wherein at least some of the information on the card is in bar code form.

12. The test request card according to claim 11, wherein at least some of the information on the card is in magnetic form.

13. A test results card for use in a system for ensuring the securing of patient's data from medical tests conducted for a medical provider by a third-party laboratory, the test results card including encrypted information identifying the patient and the results of the medical tests.

14. The test results card according to claim 13, wherein at least some of the information on the card is in bar code form.

15. The test results card according to claim 13, wherein at least some of the information on the card is in magnetic form.

16. The test results card of claim 13, wherein the results are encrypted.

17. The test results card according to claim 15, further comprising a patient identification code.

18. A method of ensuring the security of patient's data from medical tests conducted for a medical provider by a third-party laboratory, the method comprising:

issuing the patient a medical data card containing a unique patient identification number;

receiving from a medical provider a first request for a medical test generated using the patient's medical data card, and a patient specimen for use in conducting the test;

generating a second request for a medical test using the first request for a medical test, the second request for a medical test having encrypted information identifying the patient but being devoid of publicly accessible information about the identity of the patient, and including a public encryption public code specific to the patient;

forwarding the second request for a medical test and the specimen to a third party laboratory for conducting the test, and receiving the results of the test from the laboratory encrypted using the public encryption public code on the second request for a medical test;

identifying the patient to whom the results pertain, and providing the tests results to the appropriate medical provider in the encrypted form that can only be read in conjunction with the patient's medical data card.

19. A method of ensuring the security of data from patient medical tests conducted for medical providers by third party laboratories, comprising:

providing the patient with a medical data card issued by a secure information provider, having a unique patient identification number (PID), a public key encryption private key (Key 1), and a public key encryption public key (Key 2);

taking a specimen from the patient for conducting the test;

generating a first test request using the patient's medical data card, the first test request including an encrypted identification of the patient and the test; a code identifying the health care provider; the patient identification number (PID); public encryption public key; and an identification of the test type;

forwarding the first test request and the specimen to the secure information provider;

generating a second test request including an encryption of the patient's unique identification number, but otherwise devoid of any indicia that would identify the patient, and an encryption code;

forwarding the second test request and the specimen to the third party laboratory for conducting the medical test and providing the test results in encrypted form using the encryption code on the second test request;

receiving the encrypted test results, identifying the appropriate medical provider from encrypted information included with the test results; and forwarding the encrypted test results to the medical provider with an identification of the patient;

decrypting the test results using the patient's medical data card.

# METHODS AND APPARATUS FOR ENSURING THE PRIVACY AND SECURITY OF PERSONAL MEDICAL INFORMATION

## ABSTRACT OF THE DISCLOSURE

A method of ensuring the security of data from a medical test includes providing the patient with a medical data card issued by a secure information provider, and having a unique patient identification number (PID), a public key encryption private key (Key 1), and a public key encryption public key (Key 2). The medical data card is used to generate a first test request card that accompanies the test specimen taken from the patient to the secure information provider. The first test request card includes an encrypted identification of the patient and the test; a code identifying the health care provider; the patient identification number (PID); public encryption public key (Key 2); and an identification of the test type. The secure information provider uses the first test request card to generate a second test request card to forward the patient's specimen to a testing laboratory. The second test request card and the specimen are forwarded to the laboratory. The second test request card bears an encryption of the patient's unique identification number, but does not otherwise bear any indicia that would identify the patient. The laboratory performs the prescribed test and generates a first test results card. The results, together with the patient's unique identification number, are provided to the secure information provider that issued the medical data card. The secure information provider provides the encrypted test results onto a second test results card, and forwards the card to the health care provider. The test results on the second test results card are decrypted using the patient's medical data card.

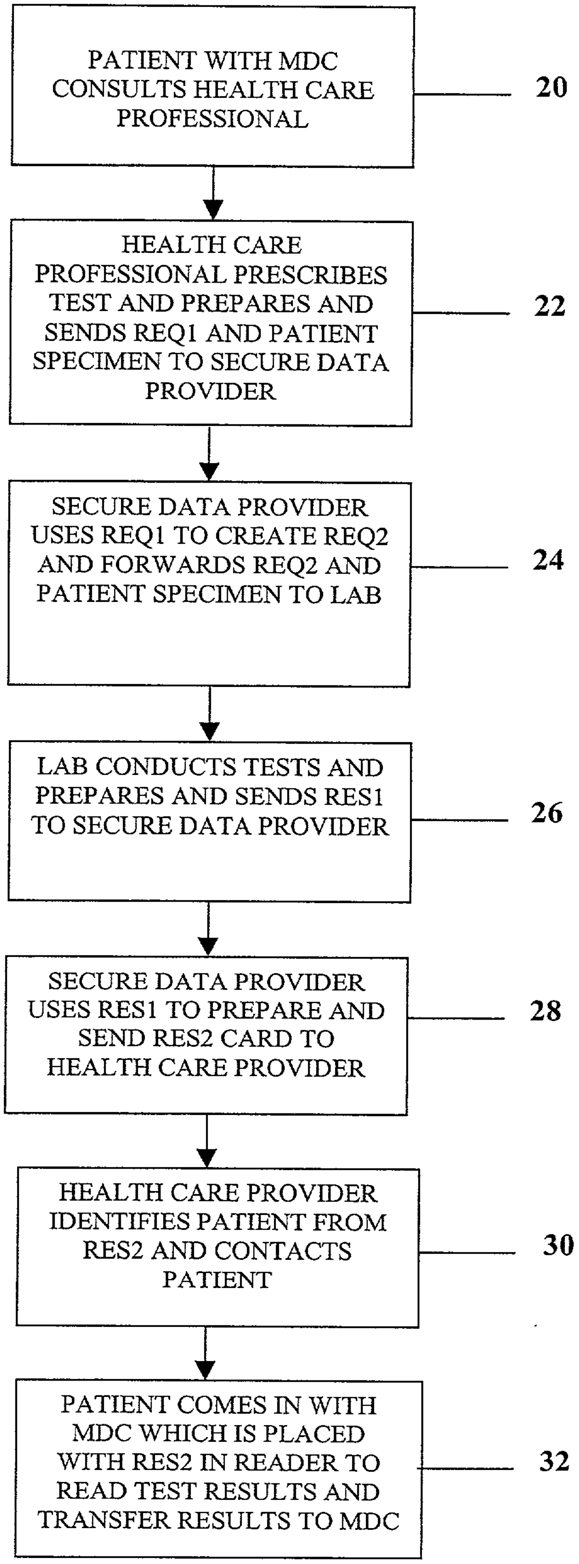
PATIENT WITH MDC CONSULTS HEALTH CARE PROFESSIONAL
20
HEALTH CARE PROFESSIONAL PRESCRIBES TEST AND PREPARES AND SENDS REQ1 AND PATIENT SPECIMEN TO SECURE DATA PROVIDER
22
SECURE DATA PROVIDER USES REQ1 TO CREATE REQ2 AND FORWARDS REQ2 AND PATIENT SPECIMEN TO LAB
24
LAB CONDUCTS TESTS AND PREPARES AND SENDS RES1 TO SECURE DATA PROVIDER
26
SECURE DATA PROVIDER USES RES1 TO PREPARE AND SEND RES2 CARD TO HEALTH CARE PROVIDER
28
HEALTH CARE PROVIDER IDENTIFIES PATIENT FROM RES2 AND CONTACTS PATIENT
30
PATIENT COMES IN WITH MDC WHICH IS PLACED WITH RES2 IN READER TO READ TEST RESULTS AND TRANSFER RESULTS TO MDC
32

Figure 1

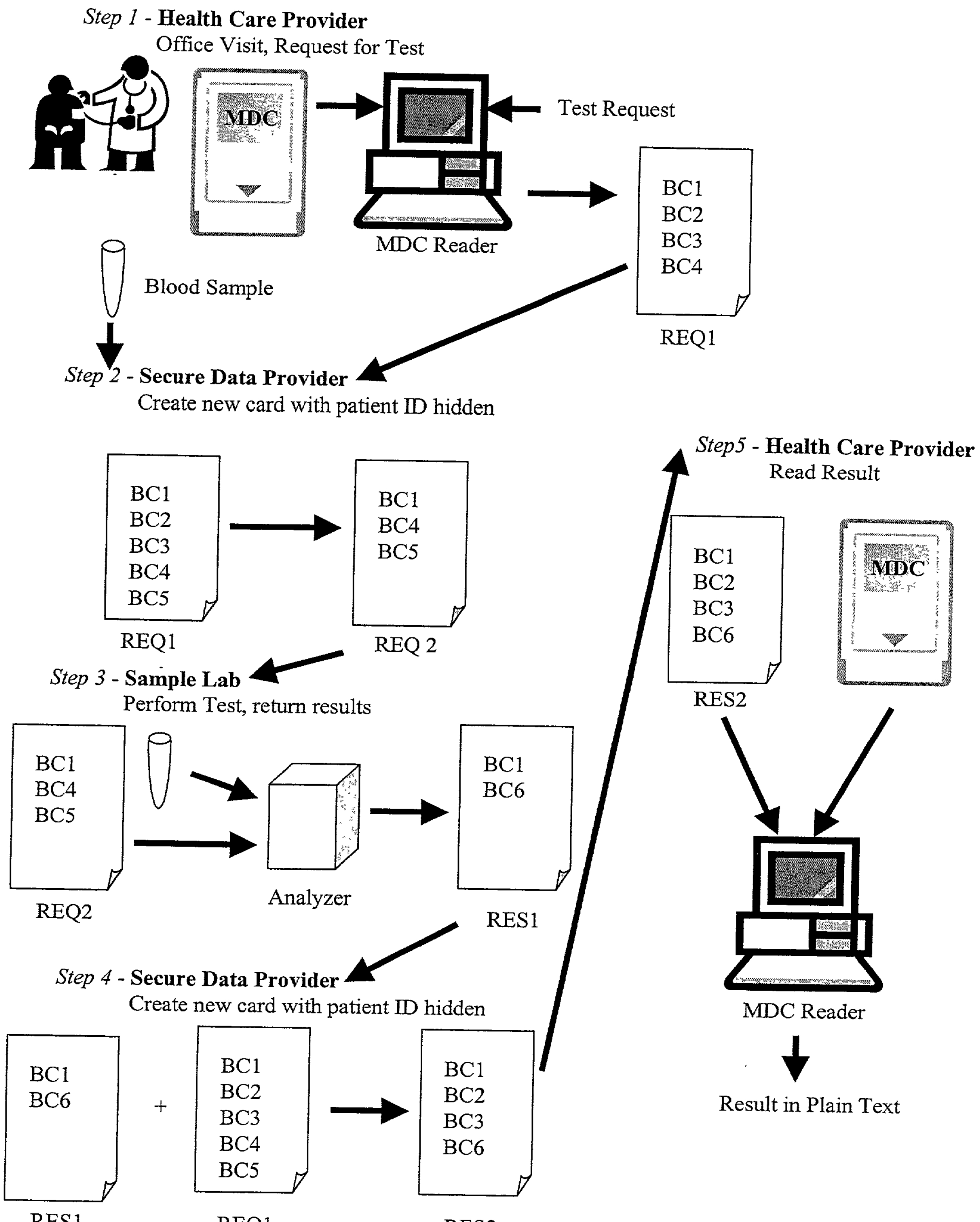
Step 1 - Health Care Provider
Office Visit, Request for Test
MDC
Test Request
MDC Reader
BC1
BC2
BC3
BC4
REQ1
Blood Sample
Step 2 - Secure Data Provider
Create new card with patient ID hidden
BC1
BC2
BC3
BC4
BC5
REQ1
BC1
BC4
BC5
REQ 2
Step 3 - Sample Lab
Perform Test, return results
BC1
BC4
BC5
REQ2
Analyzer
BC1
BC6
RES1
Step 4 - Secure Data Provider
Create new card with patient ID hidden
BC1
BC6
RES1
+
BC1
BC2
BC3
BC4
BC5
REQ1
BC1
BC2
BC3
BC6
RES2
Step5 - Health Care Provider
Read Result
BC1
BC2
BC3
BC6
RES2
MDC
MDC Reader
Result in Plain Text

Figure 2

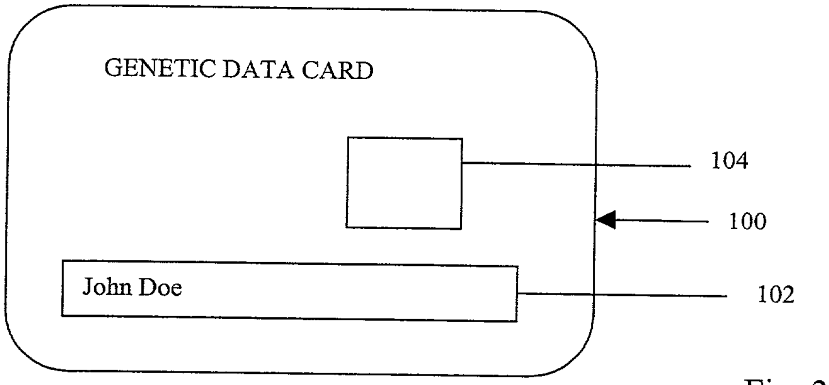

Fig. 3

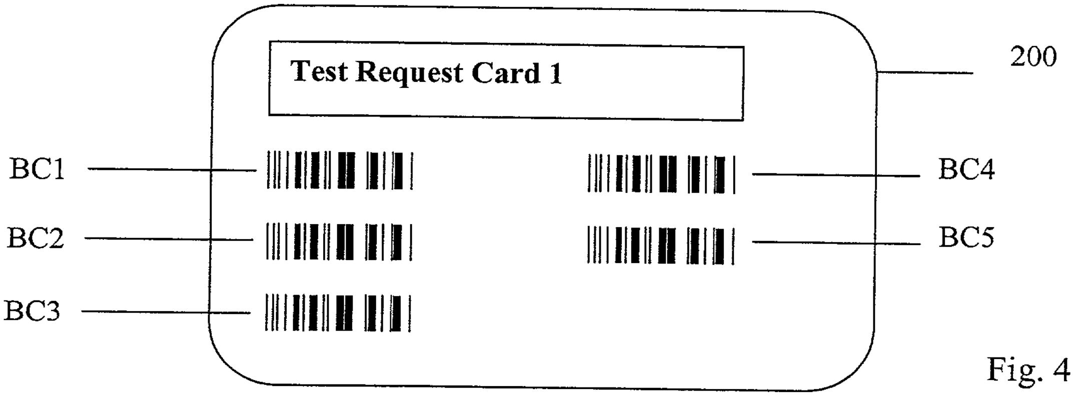

Fig. 4

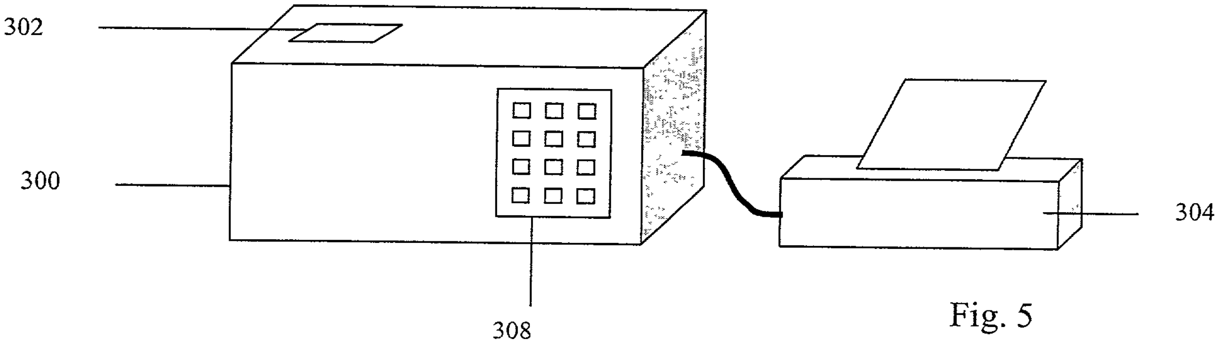

Fig. 5

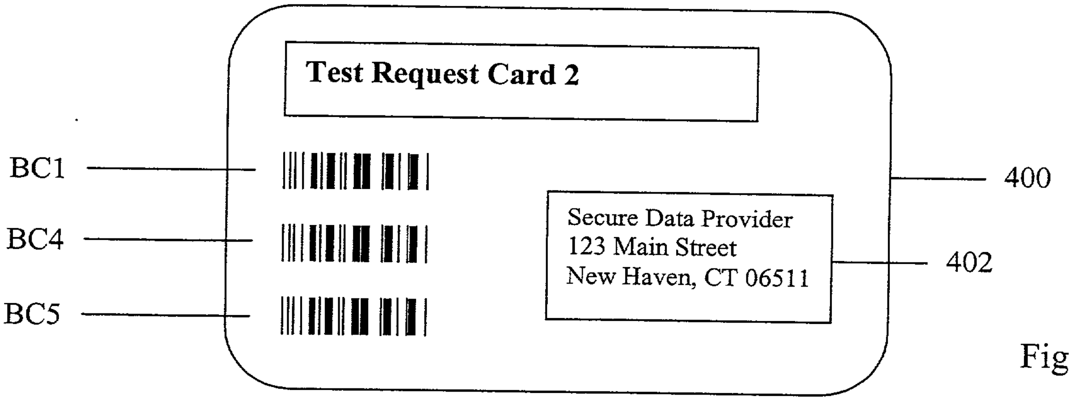

Fig. 6

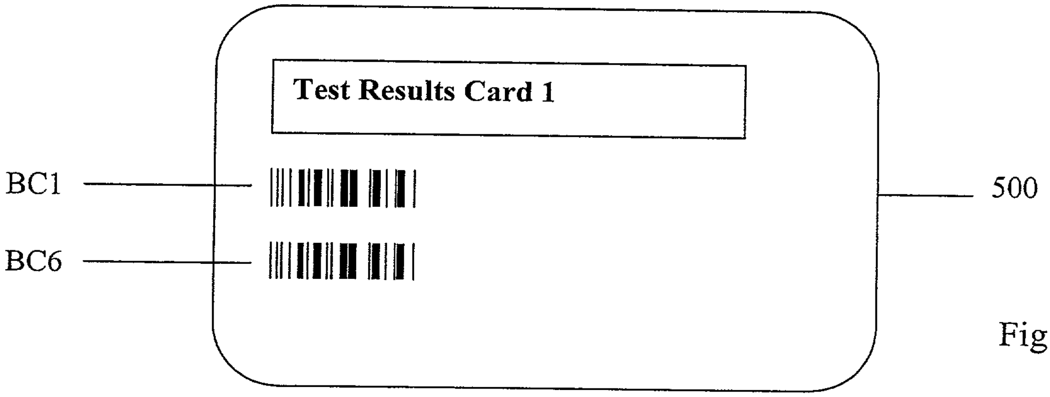

Fig. 7

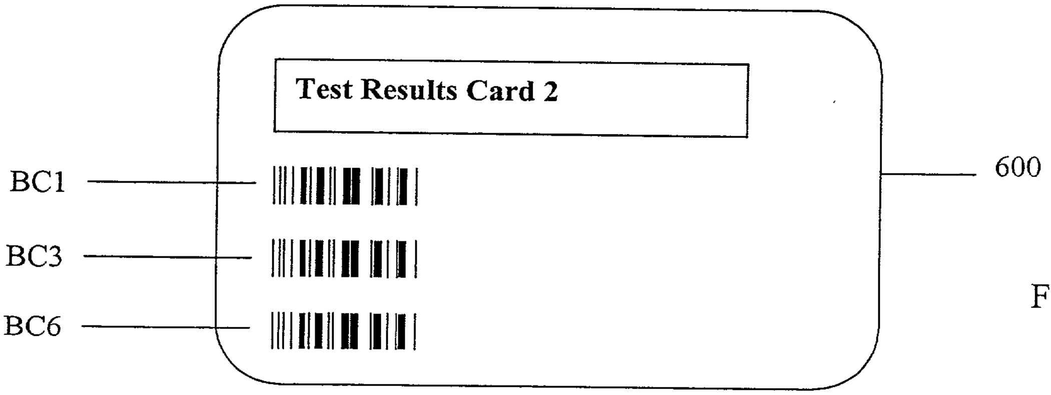

Fig. 8

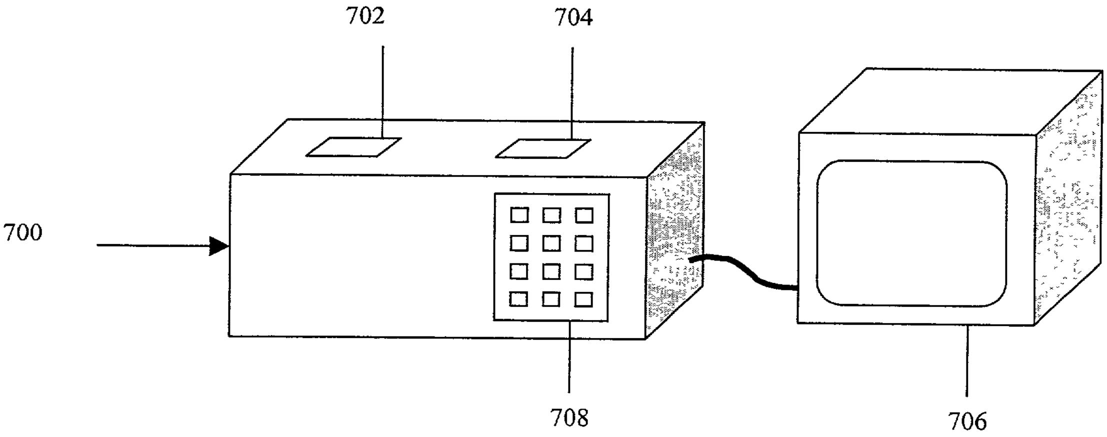

Fig. 9

## COMBINED DECLARATION AND POWER OF ATTORNEY

## (ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL, CONTINUATION, OR C-I-P)

As a below named inventor, I hereby declare that:

### TYPE OF DECLARATION

This declaration is for an original application.

### INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am an original, first and joint inventor of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

### TITLE OF INVENTION

METHODS AND APPARATUS FOR ENSURING THE PRIVACY AND
SECURITY OF PERSONAL MEDICAL INFORMATION

### SPECIFICATION IDENTIFICATION

The specification is attached hereto.

### ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, Section 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent.

# POWER OF ATTORNEY

I hereby appoint the following practitioner(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

| APPOINTED PRACTITIONER(S) | REGISTRATION NUMBER(S) |
|---|---|
| Melodie W. Henderson | 37,848 |
| Inna Shtivelband | 44,337 |

I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

SEND CORRESPONDENCE TO

Melodie W. Henderson

Customer Number 25106

DIRECT TELEPHONE CALLS TO:

Melodie W. Henderson
203-773-1450

## DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

## SIGNATURE(S)

Richard S. Judson
**Inventor's signature**
**Date** July 7, 2000 **Country of Citizenship** USA
**Residence** 42 Barker Hill Drive, Guilford, Connecticut 06437
**Post Office Address** 42 Barker Hill Drive, Guilford, Connecticut 06437